but not the name of individual users. As another example, identifying information may be recorded in a limited fashion, e.g., based on transaction thresholds and central entity requirements. As a specific example, transactions for an amount less than $1,000 may remain anonymous, while transactions for $1,000 or more may be recorded with identifying information of the entities involved.

[0150] Embodiments provide multiple advantages. As noted above, conventional cryptocurrency systems have problems such as volatility and high power usage. Many of these issues can be solved using the private, permissioned network managed by a transaction processing network and central entity to speed up and manage the flow of currency.

[0151] Advantageously, varying consensus algorithms (e.g. byzantine or crash fault tolerant) may be implemented. As a result, use of permissioned networks can provide much higher transaction throughput rates and performance, as compared to the computationally expensive methods used in traditional public networks.

[0152] Physical currency can be from markets by mimicking and digitalizing cash transactions using a Distributed Ledger Technology. The digital currency may remain tied to fiat currency and may be regulated by a central entity (e.g. a federal country bank). This can prevent the volatility associated with traditional cryptocurrency systems and allow the central entity to maintain control over the monetary system.

[0153] In addition, there is also an opportunity to prevent use and redemption of counterfeit notes and enhance security. According to various embodiments, when an entity brings physical currency to the central entity for conversion to digital fiat currency, the conversion may be denied if the serial number of the physical currency indicates that the physical currency has already been converted. Accordingly, a counterfeit alert may be issued for the serial number, that may affect both the initial conversion and the subsequent request to covert. Monitoring redeemed serial numbers can further be used to prevent use of counterfeit physical notes, enhancing the security of the monetary system overall.

[0154] Embodiments, may also enhance the security by using a chip card and/or mobile phone secure element to store private key used to sign the transactions. In some embodiments, users may store private keys associated with a given amount/value of digital fiat currency on a smart card and transfer the given amount/value of digital fiat currency to another entity by simply transferring to the smart card to the recipient.

[0155] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0156] The above description is illustrative and is not restrictive. Many variations of the invention may become apparent to those skilled in the art upon review of the disclosure. The scope of the invention can, therefore, be determined not with reference to the above description, but instead can be determined with reference to the pending claims along with their full scope or equivalents.

[0157] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0158] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0159] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

What is claimed is:

1. A computer-implemented method comprising:

receiving, by a central entity computer, a request for digital currency, the request comprising a serial number and a denomination of a physical currency;

generating, by the central entity computer, the digital currency for the denomination and linked to the serial number, wherein the generating comprises recording the digital currency on a blockchain;

transmitting, by the central entity computer, a notification of the generation of the digital currency; and

causing, by the central entity computer, removal of the physical currency from circulation in a fiat currency system.

2. The method of claim 1, further comprising:

associating the digital currency with a digital wallet using a private key stored to the digital wallet.

3. The method of claim 2, wherein the private key of the digital wallet is stored on a chip of a smart card or a secure element of a user device.

4. The method of claim 1, further comprising:

receiving, by the central entity computer from a transaction processing network, a trusted certificate for the central entity computer; and

using the trusted certificate to generate the digital currency.

5. The method of claim 1, wherein, prior to transmitting the notification of the generation of the digital currency, the recording of the digital currency on the blockchain is validated by a plurality of validating entities.

6. The method of claim 1, wherein the digital currency is recorded on the blockchain using a public key of the central entity computer.

7. The method of claim 1, wherein causing the removal of the physical currency from circulation includes physically destroying the physical currency, the physical currency being fiat currency.

8. The method claim 1, wherein the request for digital currency is a first request and the physical currency is a first physical currency, the method further comprising:

receiving, by the central entity computer, a second request for digital currency, the second request comprising a serial number and a denomination of a second physical currency, wherein the serial number and the denomination of the second physical currency are the same as the serial number and the denomination of the first physical currency;